The User's Guide to Online Safety

An Honors Thesis (HONR 499)

by

Spencer Gray

Thesis Advisor
David Largent
Signed

Ball State University
Muncie, Indiana

April 2015

Expected Date of Graduation

May 2015

Abstract

In the growing world of personal computing, a major area of concern is security. As more services move online to the cloud, the need to secure the exchange of private personal data grows. In recent years, the number of major data hacks has increased significantly, and subsequently has become a major concern among computer users. Many home users of computers however, do not understand the proper measures that must be taken to stay safe online. Many users are unaware of the different types of malware, what is considered to be malware, or how those malicious programs got on to their computer. This thesis will educate the everyday user on how to stay safe online.

Acknowledgements

I would like to thank Mr. David Largent for advising me through the process of this project. His help throughout this year and long researching and writing process is greatly appreciated, and is only a small sample of the help that I received from him throughout my time as a Computer Science Major.

I would also like thank my family for encouraging me to push through the tough portions of the work to complete this difficult task.

TABLE OF CONTENTS

INTRODUCTION

In the growing world of personal computing, a major area of concern is security. As more services move online to the cloud, the need to secure the exchange of private personal data grows. In recent years, the number of major data hacks has increased significantly, and subsequently has become a major concern among computer users. Many home users of computers however, do not understand the proper measures that must be taken to stay safe online. These users are also commonly unaware of the different types of malware, what is considered to be malware, or how those malicious programs got on to their computer.

Understanding the different types of malware and how they go about attacking your computer is crucial to staying safe online. In this thesis we will study these different malwares and their attack methods, as well as ways to avoid infection. Simple steps such as installing antivirus, properly installing software, and securing your home WiFi can lead to improved security and a much safer online experience. Gaining an understanding of these simple concepts can not only help to keep you safe online, but can also prepare you for any possible infections your computer my get in the future.

This thesis is split into sections to improve organization, and to highlight specific topics that readers may be interested in. The sections are presented in order of importance of the information, and the ease in which it can be implemented on your home computer. From here we will start by gaining an understanding of the types of malware prevalent on today's computers, and a couple of the common attacks used against everyday computer users.

MALWARE AND ATTACKS

One of the most important factors in computer security both in the home and business is malware. Many home users simply refer to having malware as having a computer virus. However, virus is not a broad enough term to encapsulate all that is malware. "Malware is software that enters a computer system with the user's knowledge or consent and then performs an unwanted or usually harmful action" (Ciampa 51). This definition shows that the term malware covers a rather broad range of possible infections. In this section, we are going to begin to understand some of the most common forms of malware that infect computers today. The types of malware we will be covering are virus, Trojans, worms, and adware. We will also cover some of the Social Engineering Attacks such as phishing and spam.

There are a few characteristics that many types of malware will show. This is especially true for viruses, Trojans, and worms. The characteristics of those types of malware help to explain how the programs get onto your computer, how they spread, how they hide, and what types of actions the malware can perform.

The circulation of malware refers to how the malware spreads to new computers. There are various ways that malware can be spread these days. Seemingly every device we use on a day-to-day basis can be connected to a home network. This allows for malware that spreads via the internet many opportunities to infect a machine. The sharing of USB drives that have malware on them, as well as through email, are also common methods of circulation malware.

The actual infection process for malware beings once circulation has allowed for the program to get on a user's computer. Once this happens, the program finds the place where it is designed to go whether it be another program, the computers registry, or even just on a bit of

memory. At this point in time, your computer becomes officially infected, and the malware is capable of unleashing its attack.

Like any good criminal, malware generally has to find a way to conceal itself once it has committed the crime of infecting your computer. There are a couple of ways that a piece of malware can hide from an anti-malware scanner. One way is for it to hide within another program allowing to run within the program's process thus looking like legitimate software. Another way malware can hide is actually editing the operating system of your computer. This is essentially the malware making itself a part your computer's operating system. This form of concealment is less common, but it very difficult to fix if it happens.

The payload of any type of malware relates to what the malware is trying to accomplish. This could include stealing data, deleting important files, or changing settings to allow another attack to happen. Some types of malware focus solely on having a large payload capacity and are often found by scanners. The trouble is often times the malware has already done damage before a scanner can recognize it.

VIRUSES

The first type of malware we will discuss is also generally considered the most common. A virus is a type of malware that generally will insert itself into a file on your computer, and is then executed when the program it has attached to is used. The term virus is used to describe this type of malware because of the way it replicates itself. Much like a virus in the human body, computer viruses replicate themselves and move between files on your computer. They do this without any kind of command from the user. This allows for the circulation of a virus to happen without the user realizing there is a problem. Once fully embedded on a user's computer, today's

viruses are capable of deleting vital information, causing constant computer crashes, changing security settings on the operating system, or even formatting the drive entirely.

Early computer Viruses did not start out with these advanced capabilities. According to Nikola Milošević on page three of his article "History of Malware" the very first piece of malware known to infect Windows was WinVir. It worked by finding the Windows Portable Executable files and infecting them. When the infected files were run, WinVir found new files to infect and rolled back the formerly infected files. This means that the virus was deleting itself as it moved between files. It was from these humble and non-harmful beginnings that today's computer viruses came to be.

TROJANS

The next type of malware is the Trojan. Trojans are named for the way they enter a computer. When these malicious programs are installed on your computer, they act as if they are a simple harmless program that performs a simple task. This is much like the horse the Greeks gave to the city of Troy with soldiers hiding inside. An example of this given in Ciampa's *Security + Guide to Network Security Fundamentals* is a user installing a program that claims to be a simple calendar creator, but in reality it has malware that scans the computer looking for credit card numbers and passwords while being connected to the internet to send the information to the attacker. One important fact to get out of this is that the user has to take the action of installing the original program for the Trojan to get on the computer. Trojan's also require the user to move the files to other computers in order for it to spread.

WORMS

Worms exist primarily to spread themselves. "A worm is a malicious program that uses a computer network to replicate" (Ciampa 57). Essentially a computer worm is designed to get onto a computer via the network it is attached to. It will find a vulnerability on the system, and use it to infect the computer. Once it has done this, the worm begins a search for yet another computer on that network. If it finds one that has the same vulnerability, it will replicate itself and move to that computer.

The original worms were only designed to do this replication. They would be sent out to infect as many systems as possible, however they contained no payload, thus not causing harm to the infected computers. The only effect they had was to slow down the networks in which they were running. These worms replicated so quickly that they were using all of the available bandwidth on the networks (Milošević 5-7).

Today's worms have grown to be much more malicious. Once the worm has made its way onto a computer it now contains a payload that allows it to potentially cause great harm to a machine. The effects of today's worms are very similar to that of a standard computer virus, the difference being their ability to spread to a large number of computers quickly. One of the most significant worms in recent history is the Love Bug or ILOVEYOU worm. This piece of malware was sent via email, and if the user were to open it, the computer became infected, and most files on the machine were overwritten. The circulation of the worm was effective because it searched the machine for outlook contacts. Once found it would send an email to all of the contacts. It is estimated that the worm caused somewhere around 8 billion dollars of damage (Knight 1). Today it is common for many attacks to be sent via email.

SOCIAL ENGINEERING ATTACKS

Social engineering attacks are designed to take advantage of the weaknesses of people. Ciampa describes a situation in which a group of people were able to walk into a company, take valuable information from the CFO's computer and gain full access the network by simply relying on human weaknesses. They used techniques such as saying they had lost their key, calling human resources for basic information, and impersonating the CFO in order to pull this off. This example was used to show that a person doesn't always have to be a master hacker to gain access to a system or network.

PHISHING

One of the most common types of social engineering attacks is known as phishing. Phishing uses the trusting nature of people to get personal information from users. To do this, an email is sent to a user that looks to be a legitimate business such as PayPal or Amazon. In the email, the user is asked to update information such as their credit card numbers, password, Social Security Numbers, or even bank account numbers. If the user follows the given link they are taken to a fraudulent website where they can enter this information. Once entered the information is sent back to the person in charge of the phishing. At this point the attacker has access to all of the information that was given to him.

The reason phishing is so common, and seems to continue working is that the emails sent look and feel like they are from the actual company. The email and site link will commonly have the logos from whatever entity they are claiming to be. It is important as a user to always question these types of emails. Even when they sounds very urgent, it is best practice to go through the actual website to update any information rather than using the link provided in the

email. If the website has no notification telling you to update this information, the email is mostly likely a phishing scam.

Recently a phishing attack known as "the Fappening" made the news. In the attack, celebrities such as Jennifer Lawrence and Kate Upton were targeted with a phishing attack in an attempt to gain access to their iCloud® accounts. iCloud® is the online storage service offered by Apple for storing photos and videos from users Macs®, iPads®, and iPhones®. The celebrities entered the information after following the link in the email, and this gave their login information to the attackers. Later, all of the photos found were leaked to the internet including many sexually explicit photos. This has led to many lawsuits and lack of privacy for the celebrities involved. This is proof that a phishing attack can happen to anybody, and any email asking you for personal information should be handled with caution.

Spam

Spam is another very common form of social engineering attacks. "Google estimates that 9 out of every 10 email messages are spam" (Ciampa 71). The reason for spam is not to infect a computer with malware, but instead is based around making money. Fake products or deals are offered in the emails in the hope that users will pay thinking the email is trustworthy. By using a botnet, which is a large group of computers controlled by a single attacker, spam email can be sent to millions of users in very little time. If even a fraction of a percent of the users fall for the scam, the spammer will be able to make hundreds of thousands of dollars in profit.

Some of the most common examples of spam will focus on the insecurities of male users. The emails will offer a deal on an erectile dysfunction medication such as Viagra, or even a miracle cure to some other male problem. Since many males in the world are insecure about this,

they are more likely to fall for the scam and pay for the items the deal is claiming to have. It is important when looking at an email about a deal to see if it includes some of the signs that the email is spam. These signs can include a subject line like "Check This Out!!!" or "You Can't Miss This Deal," the words in the email are in an image, or there is text at the bottom of the email that doesn't make sense.

These are just a few of the types of malware and attacks that can be executed on a computer. Many computers are infected with malware every day, so it is important to understand the types of malware and their risks. It is also important to keep in mind the type of infection you have when deciding if you should try to repair your computer or take it to a technician. Taking the proper steps to repair an infected computer are important. Sometimes it takes the expert skills from a computer technician to remove the malware. Other times it is possible to use a simple malware removal tool to remove the infection.

ANTIVIRUS AND MALWARE REMOVAL

One of the biggest worries for computer users is staying protected from malware. In the previous section, we discussed common types of malware, how they spread and infect, and a couple of common attacks. After learning about the dangers of malware, it can be difficult to feel comfortable with your computer's security while online. Luckily there are antivirus programs that can help keep you safe, and malware removal tools to destroy any malware that might make it onto your computer. In this section we will be discussing how to install and setup the free antivirus software Microsoft Security Essentials, and how to use two common malware removal tools in the even that your computer becomes infected.

ANTIVIRUS SOFTWARE

As a user, it is important to keep your personal information and files safe by preventing the infection of viruses and other types of malware. Surprisingly, many users do not understand the importance of antivirus software. Those who do understand that it is needed do not always know how to install and configure it to keep them safe while online. According to the June 2014 Microsoft Security Intelligence, around 20 percent of computers have less than adequate security software, and are at times left virtually unprotected online. Installing proper security software is one the first and most important things to do on any computer.

There are many free and paid security software suites available for Microsoft Windows operating systems. Most computers sold in stores come with a free trial of Norton Internet Security, however many users let the subscription end and choose not to renew. Once that subscription ends and the software stops updating, the computer's security is no longer adequate and is at risk and the computer is vulnerable to attack. The simplest solution to this is to uninstall

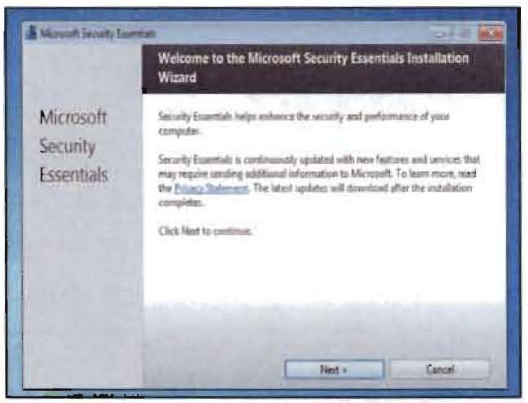
the outdated software and install a new free one that will stay up to date and keep your computer protected. It may seem simpler to leave the outdated software on your computer, but this will hurt the performance of your computer, and will not increase your security. Choosing a free software for your computer can be confusing due to the high number of options available online. The three most common choices are AVG, Avast, and Microsoft Security Essentials (MSE). Generally deciding on which of these software options is best is a matter of opinion. For the purposes of this guide we will be installing MSE.

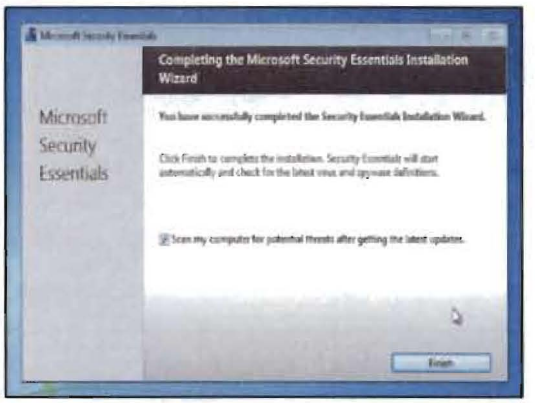
The first step toward securing your computer is to remove the outdated antivirus software currently installed. To do this, click the start button and go to control panel. Once in Control Panel, select "uninstall a program" under the "Programs" section. This will lead you to a list of programs currently installed on the computer. Find the outdated software in the list and double click it. The uninstall manager for the software will then be displayed on your computer. Follow the uninstall instructions in the manager to completely uninstall the program. After uninstalling your outdated antivirus software, you are ready to download and install MSE.

To get the install file for MSE simply search Google for Microsoft Security Essentials and click the link directing to the Microsoft website. The website will automatically choose the version of the software appropriate to your operating system. Just click Download Now and locate the installation program in your computer's downloads folder. Once you have the file downloaded, it is time to begin the install process.

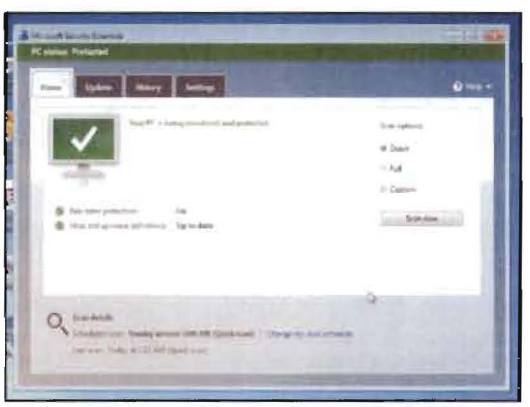
Run the .exe file and the install screen will appear. Since we have downloaded the software from Microsoft, there are no extra programs attached to the installer so the install process is very simple. Simply follow the prompt by selecting "next" until you get to the final

screen then click finish. At this point you have successfully installed the Microsoft Security Essentials software.



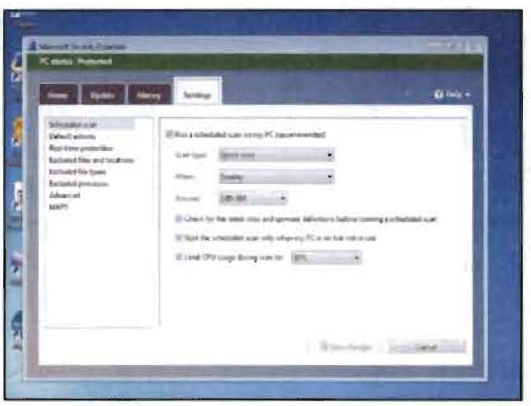


After the installation process is complete, the software will automatically start and update itself. If you left the box circled in red above checked, a preliminary scan will be run after installing the latest updates. The first scan will inform you of any viruses or other malware found on your computer. If this install process is done with a new computer, MSE generally will not find any malware on the computer. After the scan is finished and nothing is found, you will be presented with a screen saying "Your PC is being monitored and protected."



Now that your computer is being protected by security software, it is important to set up a scheduled scan of the system. Running scans regularly can help to alert you of any possible

malware before it has had a chance to harm your computer. By default MSE will set a scheduled scan for Sundays at 2:00AM. If this is a time in which you will be using your computer, or it will be turned off then it is important to change the time of the scheduled scan. A scan can be run while the computer is in use, but a slight drop in performance during the scan might be noticed. To change the scheduled scan settings, go to the settings tab of MSE. From here, many settings can be changed, but many of the default settings are good for standard home use. When changing the scheduled scan you are given the option to run a quick or full scan, as well as the ability to choose when the scan will be done. If you are going be to on the computer during the time of the scan, running a quick scan might be the best option. However, if you will be away from the computer it is a good idea to run a full scan of the system.



With security software installed and the settings optimized, you are protected from most malware when searching online. However, even with the best security software, it is possible for malware to find its way onto your computer. Improperly installing software, downloading and running infected files, opening infected emails, and clicking on certain pop up adds are just a few of the ways malware can get onto your computer. Most security software such as MSE is designed to block known malware, but is not designed to completely remove the malware if it has made it onto your system. To remove malware, a malware removal software is needed.

MALWARE REMOVAL

The removal of malware is a task commonly left to the talents of a skilled computer technician, or simply not done at all. Taking your computer to a repair shop can get expensive, and most common forms of malware can be removed with a couple of simple tools. Malware removal software such as Malwarebytes and ADWcleaner (ADW) are designed to locate infected files on your computer and delete or repair them. Most malware coming from installing software from free download sites and similar sources are designed to annoy the user and collect data. Using the proper malware removal tools can repair your computer and save your personal data. It is important to keep in mind that some malware is extremely difficult to remove and may require the expertise of a technician. The two pieces of software being discussed are great for basic users because running them will not harm your computer. Other types of malware removers can delete system critical files if used improperly. A general rule of thumb to follow is that if Malwarebytes and ADWcleaner don't remove the malware, then a trained technician is likely needed.

Malwarebytes is a very well rounded piece of software. Both a free and premium version are offered. The premium version offers many great features such as real time protection to go along with your antivirus program, but for the purposes of malware removal the free version will do the job. An important note when installing the free version of the software is that you will need to uncheck the box asking you to use the free trial of the premium features. Without unchecking this box, you will be given premium for one month, and then asked to pay to continue the service.

To install the free edition of Malwarebytes, download the install file from Malwarebytes.org. Make sure you chose the free download option. After downloading, double

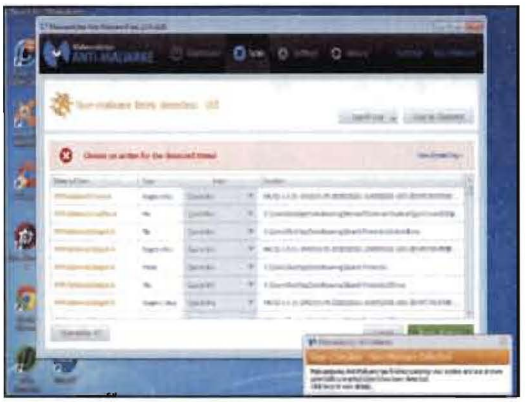
click the install file and follow the instructions. Since the install file was downloaded from the official Malwarebytes page, no extra software is attached, allowing you to simply agree and click next until the final screen of the install. The final screen includes two check boxes. The first asks if you would like a free trial of Malwarebytes Premium. This box should be unchecked before clicking finish. The second can be left checked, as it allows Malwarebytes to run after installing. After clicking the finish button, Malwarebytes will be installed, and the malware removal process can begin.

Once installed, running Malwarebytes is very simple. To start a scan, you simply press "Scan Now," and allow the program to run. You may be asked to update the virus definitions before starting the scan. It is important to allow this update to happen in order to make sure the malware will be able to be removed. Once scanning, Malwarebytes will run through six different phases. These phases allow the scanner to search in all possible locations for any malware on your machine. It is important to allow the scan to run to completion. It is not uncommon for the scanner to find remnants of malware on the system at the very end of the scan.

During the scan a dialog box can be opened to view what has been found. This box is generally only useful for computer technicians, as they can tell the severity of the infection based on what is displayed. The number of items found can quickly grow to over 100 due to the in-depth nature of the scan. This does not mean that there are hundreds of different types of malware on the computer. Each single instance of malware can have many different files and remnants associated with it, and each one will count as a separate item found. Most scans will last between five and twenty minutes, but heavily infected or older computers can take much longer to scan.

Once the scan has completed, Malwarebytes will display everything that it has found on the system and ask how you would like to handle each item. The two options are to ignore or quarantine the files. The reason Malwarebytes does not delete the files is that an important file might be detected as an infection and need to be replaced. Quarantining the files allows for them to be restored without harming the computer further. Some items found may be listed as "Non-Malware" or "PUP" files. PUP stands for potentially undesirable program. These files are ones not considered to be malware, but should still be removed from the machine. If you do not wish to look through each files, there is an option to quarantine all files. The scan is then completed and all files found during the search are safely removed from the operating files on the computer.

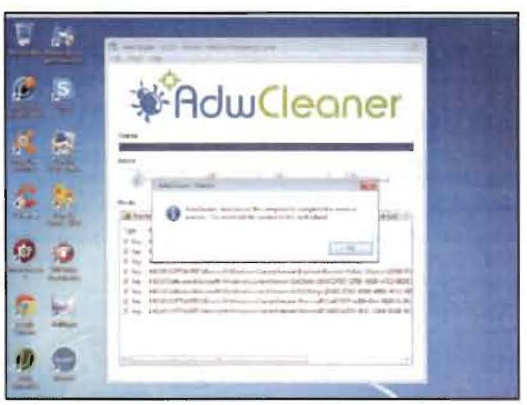
Malwarebytes will tell you that the cleaning process has completed, and give you the option to view a log for further details about the files removed.

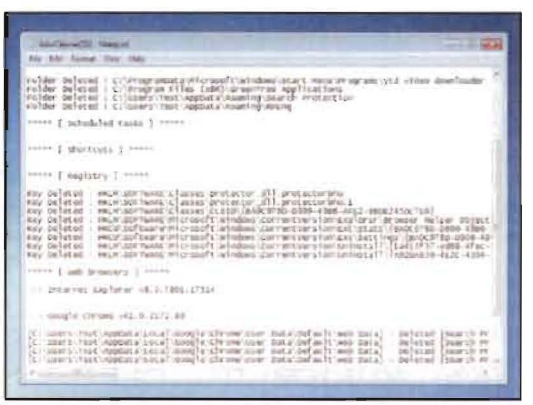


For many infected computers, one scan is not enough to remove all malware on the system. ADWcleaner is another strong malware removal tool. The ADW in ADWcleaner stands for Adware. ADWcleaner is designed to focus specifically on Adware and PUP files, while Malwarebytes is a generalized overall scan. ADWcleaner is a great tool to use after running Malwarebytes, as it will work to remove programs from your computer that were not recognized as Adware. Since ADWcleaner is very specific in its search, it generally runs very quickly, and gets off most or all adware. There is no installation process for ADWcleaner. Simply download the .exe file from BleepingCompuer.com. Running the .exe will run the program.

To run a scan with ADWcleaner simply open the program and click the scan button. Any updates will run automatically, and the scanner will search in locations known for adware. Once the scan in completed, you can look through the results to see what was found. Each item found is separated into different sections to make reviewing the scan simpler. The sections are services, folders, files, shortcuts, scheduled tasks, and registry. There are also sections displaying items found in the files of the internet browsers on the computer.

After reviewing the items found during the scan, pressing the "cleaning" button will start the cleaning process. Since the items found by ADWcleaner are known adware files, the items are completely deleted from the computer to insure reinfection will not be a problem. To fully uninstall the programs and delete the files, ADWcleaner will warn that the computer needs to be restarted. Upon clicking "Ok" in the dialog box, the computer will be restarted, and all files adware files found will be deleted. After the computer has been restarted, a text file will be displayed to show all of the content that has been removed from the computer. The file is saved on the "C" drive of the computer, and can be left there for further review as it takes little space. Leaving the files on the computer can help computer technicians understand past infections on the machine if they are doing a malware removal service.





After running these two scans, most malware infections will be removed from the computer. It is important to remember that some infections can be more serious, and these scans may not completely solve the problem. If after running these scans, there still seems to be malware installed on the computer, or performance has not improved, taking the computer to a technician is probably the best option. They will have much stronger tools to remove any other infections, as well as scans to check if other problems are present.

Running antivirus on your home computer is a great way to keep it safe from virus, Trojans, and other types of malware. Having a scheduled scan can warn you of infections on the computer before they have had time to spread, and can sometimes stop and remove the malware in its tracks. Other times, malware removal tools such as Malwarebytes and ADWcleaner are needed to clean the infections out of the computer. Having a basic understanding of these tools can help to keep personal information and files safe.

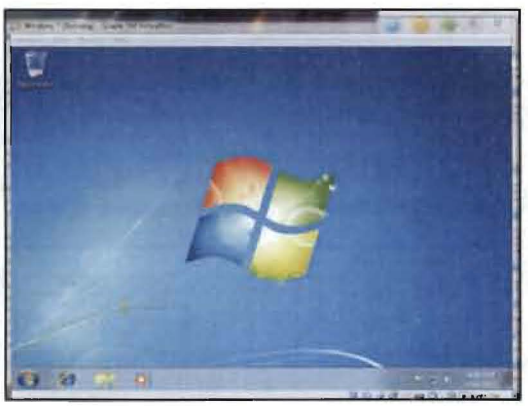
INSTALLING SOFTWARE

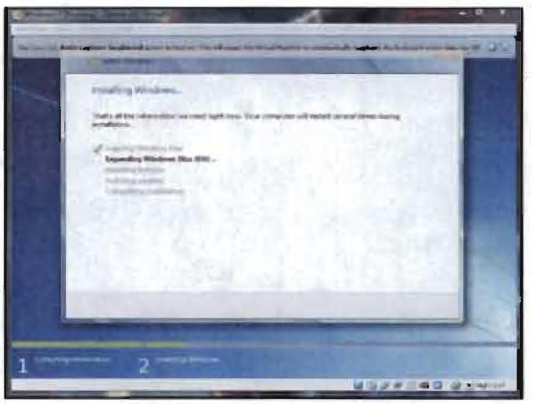
Installing software on your computer is one of the most essential abilities every user must have. Most users have the basic idea of clicking next until their next piece of free software has been installed, and is up and running. The trouble is, clicking next quickly can allow for too much software to be installed. A general rule of thumb to consider is this: if a website is offering you a free pieces of software created by other companies, then the software will cause more trouble than it will actually help. Websites that offer these free programs such as Download.com have to make money to keep their website up and running. To do this they offer free programs that come with other programs attached to them. These hidden programs are generally types of adware or even contain a Trojan that could harm your computer or even take personal data.

A recent article online from howtogeek.com titled "Here's What Happens When You Install the Top 10 Download.com Apps" describes and tests a scenario that shows the effects of an uneducated user installing software through one of these sites. The idea was to go online and install the top ten downloads from Download.com. The rule was that during the install, only the next and accept buttons could be clicked during the installation. This would allow the installer to add all of the extra software to the computer. Essentially, by the end of the article it was clear that the computer was heavily infected.

For the purpose of education, I have decided to recreate the experiment. My goal for this experiment is to show that understanding how to properly install software is important. The only difference is that I am only going to be downloading five of the most common programs. Also, after reading this section, you should better understand the importance of reading what you are agreeing to before clicking the "OK" button. To show how much damage could be caused by

downloading software from the wrong source I started with a clean install of Windows 7 on a virtual machine. A virtual machine is a computer that runs via software. It is hosted on a physical computer, and is essentially a separate program running on the host computer.

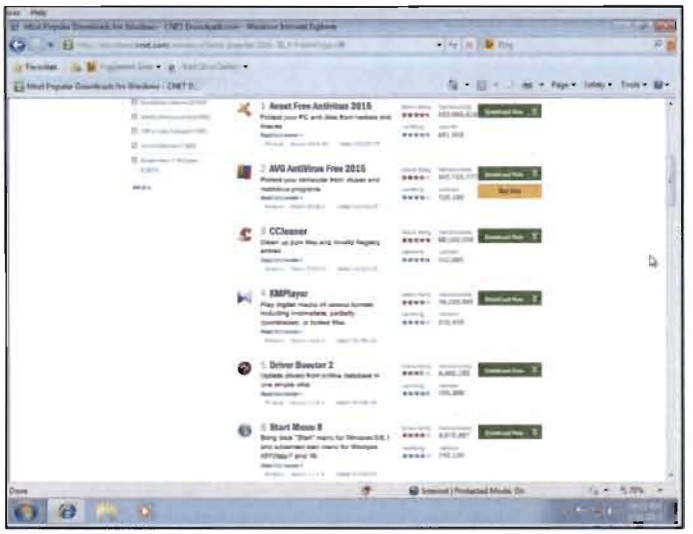




As you can see from these pictures, the virtual machine had a truly clean install of Windows 7 with no extra programs installed. I then proceeded to Download.com, and went to the most common downloads to see what I would be installing on this machine. One thing to note before the first applications are installed, is that the original homepage of Internet Explorer is MSN.com and the original search engine is Bing.

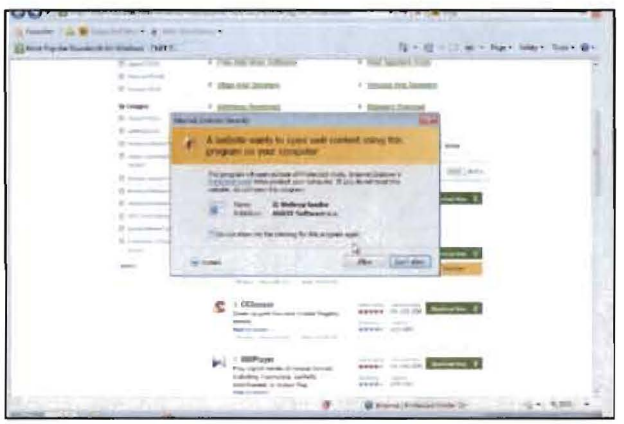
Upon getting to the popular download page, I noticed a few things. The first thing that caught my eye was that the top two downloads were both antiviruses. I decided it best to skip the second

antivirus and chose another piece of software. I also noticed that a couple of the programs are actually quite trustworthy when downloaded from the actual author's site. I use a couple of the programs myself. I also decided to skip number six on the list as it did not pertain to Windows 7.



From here it was time to begin installing software on the computer. The number one most popular download from the site is Avast Free Antivirus. I am glad to see that this was number one. The good news is that many users of Download.com are concerned about their safety online. Avast is a well-known antivirus that is trusted in the community of computer technicians. Having personally installed it many times, I knew there was one program attached to it, so I was not surprised by the install process.

After downloading and running the file from Download.com you are eventually led to this screen. This is the first point at which you are agreeing to install software other than what you have downloaded. Circled in read are two check boxes. Leaving these boxes checked means you agree to install the extra software attached to the installed. Luckily Avast simply has Google Chrome and the Google Toolbar attached. Neither of these are harmful, however toolbars will slow down your internet browser. Though after the install is complete we are asked to accept the installation of an add-on for Avast. Couldn't hurt if our anti-virus is asking for it right? In this case we are fine, but popups like these are one of the many ways extra files and programs are installed on your computer.

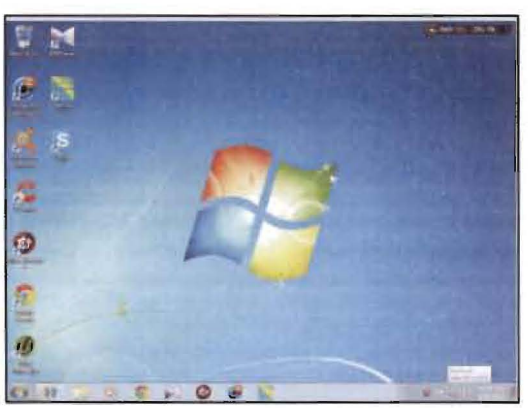


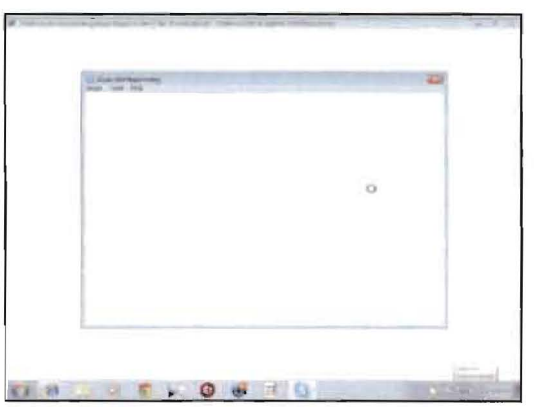
After the installation of Avast and subsequently Google Chrome, I moved to the next piece of software on the list. At this point I installed CCleaner and nothing extra was installed with it. Sometimes downloads go smoothly and nothing extra is added. So at this point after two installs we have three new programs and no noticeable performance issues. That however is soon to change. Next up on the install list is the KMplayer.

KMplayer is a media playing software that can be used as a replacement for Windows Media Player. The program itself is not in any way harmful to your computer. The problems start with some of the software that is attached to the media player as well as some of the other programs that I will be installing. The install process for KMplayer seems harmless, but much like when installing Avast there is a specific screen in which you are asked to agree to install software other than what you are trying to install. Below you will see the process in which most programs coming from Download.com are installed, as well as the point of the install in which you agree to install more software.

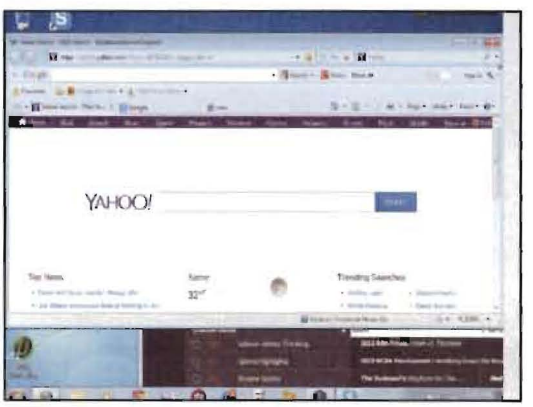
This is a very common install process for Download.com software. Circled in red is the point in which you are asked to agree to the install of added software. Some installs will ask for permission multiple times. The more added software included in the download, the more money the website makes off the install. One good thing that came at the end of this install is Avast doing what it is meant to do. The warning displayed is Avast saying it has blocked a file or program is recognized as malware from being installed onto the computer. This is a clear example of how anti-malware services are beneficial to a computer.

For the remainder of the software, I followed the same process of installing software while clicking accept to every option like a standard user. It was clear after the install of the KMplayer however that I was going to have a lot of extra software. The remaining pieces of software to install were Driver Booster 2 and YouTube Video Downloader. Both of these programs are completely unneeded and generally a very good idea to stay away from. I installed the driver program next, and was given a couple of options to install more software. After saying yes and allowing the install to run completely, I was up to nine programs now installed on the computer. Remember this is after choosing four pieces of software to install. Also, I am beginning to notice major performance issues and freezing as more software attempts to install itself.





By the time I finally got the fifth and final piece of software installed, the computer was up to 12 programs installed, had software set to run on start that I never actually installed, and was facing boot times of three to four minutes. With this being a virtual machine, I was originally getting boot times of around one minute. Another problem I noticed was that my homepage and default search engine had been changed to Yahoo. I also now had three different pages loading when starting Internet Explorer. This caused the browser to run very slow. It is clear that after five free programs and all of the extra things attached to them, this computer struggled to run properly. This is the point when most users would complain about the speed of their computer and either look for a new machine or take it to get repaired. Luckily in the malware removal section of this guide you can find a step by step guide to removing the malware installed on this computer. The other thing that can be done to help improve the performance of the machine is to uninstall programs that are unneeded or were installed as an add-on for the software you wanted.



Now the once cleanly installed virtual machine is full of garbage software, malware, and adware. The important take away from this is that free download sites are not the safest place to get new software for your computer. Search for the software that is going to accomplish the task you are looking to complete and install it from the creators actual website. The other important

idea is that when installing software it is always important to read what you are agreeing too before selecting agree or next. Most of the extra programs that were installed and the search engine changes could have been avoided by simply reading and selecting disagree. It may take some extra time to read all of the screens during install, but in the end it will save you time and effort when your computer continues to run well.

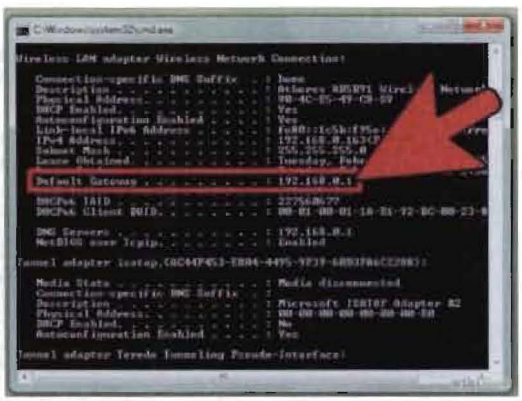
SECURING YOUR HOME WIFI

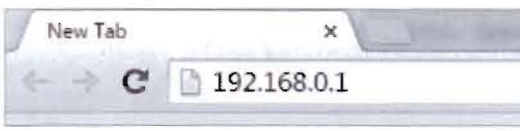
According to the Census Bureau in 2013, 74.4 percent of households in the United States had access to the internet, while 73.4 percent had access to internet that could be considered high speed. Recent trends in technology also show that wireless internet connectivity is becoming the most commonly used option for internet access. With more homes gaining access to internet and WiFi technologies, it is important to understand the need for wireless security in your home. Most routers sold at retail stores put emphasis on ease of use and quick setup. Simply plug them into the outlet, connect the Ethernet cable form your modem, and sign on. The step that is not commonly mentioned is going into the device settings to make sure your home network is protected. There are a few basic settings changes that can be made to make sure you are secure. In this section we will discuss the process of getting to the setting on your router, and setting them to be secure.

It is safe to assume that upon purchasing your new router, you simply plugged it and connected your favorite wireless to the wireless internet. However, now that you are connected, it is time to change the security setting on your router. The screenshots in this section come from an article on wikiHow that also describes securing your WiFi, as well as the Linksys routers website. The wikiHow article gives steps that can be too advanced for some users, so we will be focusing on some of the most important steps.

The first step is logging into administrative features on your router. This process is different than singing onto the internet. Once you are online, you have to find the Gateway IP address of your router. This "gateway" is the address of the router's home screen. To find this address you will need to use the command prompt on your computer. The steps to do this are:

1.) Click the Start button
2.) In the Search box type CMD to find and run the Command Prompt
3.) Once in the prompt, type the following: ipconfig /all then press enter
4.) Scroll through the newly displayed text to find the line labeled as Gateway and copy that address
5.) Open your internet browser and enter the address into the address bar and press Enter

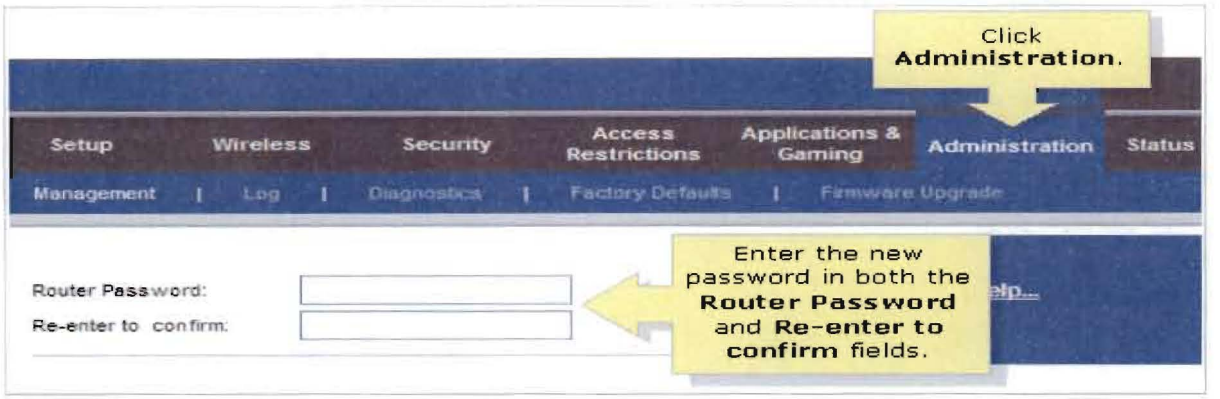




After you have entered the address and pressed enter, you will be redirected to the login screen for your router. The default username and password will be listed in the in the documentation included with your router. If you do not have the documentation a simple Google search can be done to find the information. For many routers, the default username is "Admin" and the default password is "administrator." With the default login information being so easy to find, this is obviously one of the settings that will need to be changed. This is one of the easiest settings to change, and can offer much greater security on your network. The example shown below is from a Linksys router. Other brands of routers will have a very similar method of changing the password on your router. The steps are as follows:

1.) Log in to the router via the Gateway Address
2.) Select the Administration Tab
3.) Under the Administration Tab Enter and Re-enter the new Router Password

4.) Click Continue, and the password has been changed.



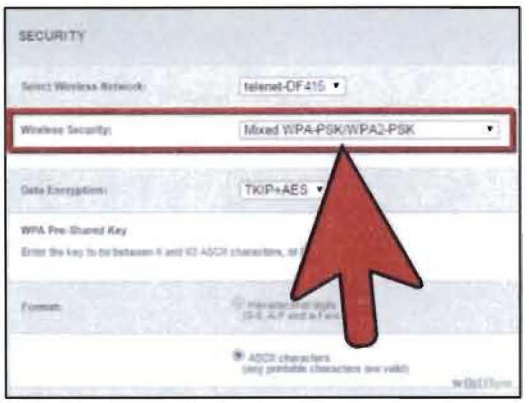
There is another password set to your router that you have already used. Today's routers come with a default password for logging into internet connected, as well as a default setting for the encryption being used on the password. After changing the administrator login information, it is important to make sure that the access password has been changed, and the encryption is set to WPA2. The concept of what type of encryption you are using in an advanced topic, but the basic idea to remember is that WEP encryption can be broken rather easily but WPA2 is much stronger. On some routers the encryption setting will be set to WPA2 by default, but it is important to check this, and to change the default password. The steps to changing these settings are simple to follow.

Encryption Settings

1.) Log in to your router
2.) Select the Security Tab
3.) Under Wireless Security choose WPA2
4.) Click Ok and the Setting has been changed.

Change Default Password

1.) Log into your router
2.) Select either Security or Gateway tab (Name of tab will depend of brand of router)
3.) In change password section Enter the old password, new password, and re-enter new password
4.) Accept the changes and the password has been changed.

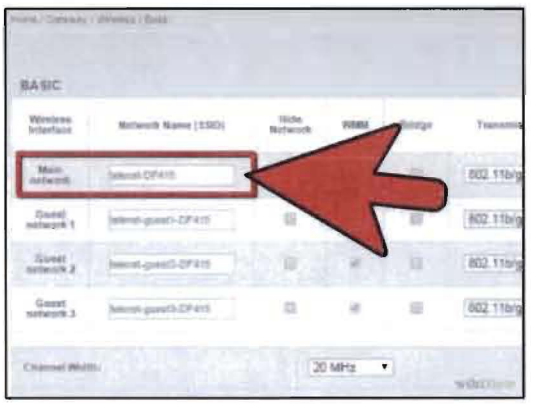


Choosing a secure password is important when changing the internet access password for your home network. A password such as abc123 or password can be easily guessed, and will give an attacker access to your network. Best practice is to choose a password that is at least 10 characters long, doesn't repeat characters, and has numbers, letters, and symbols included. If you are concerned about choosing a proper password, password generators are available online, and will give you randomly outputted string of characters to use as a password. Keep in mind when setting a password that you will need to be able to remember the password for connecting new devices to the WiFi.

Another basic setting to change is the SSID for the router. This is the name that appears in the available wireless networks on windows. By default, the name is generally the model number or manufacture name of the router. Leaving this set to the default is a red flag for attackers searching for a router that has default settings loaded. Even if you have taken the time to change other settings, changing the SSID on your router can stop a rouge attempt to access your home network before it even begins. Generally the option to change this ID is in the basic settings tab for the router.

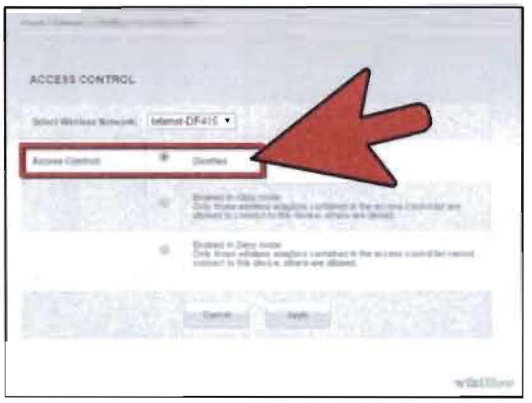
1.) Log in to your router.
2.) Select the basic settings tab
3.) Locate the field tiled SSID

4.) Change the name so something signifying your home network such as AdamsFamilyWifi
5.) Accept the changes



After changing all of these settings there is still one more important change to make. Even with a very secure password, a changed admin password, and custom SSID it is possible for someone to gain access to your home network. The attacker could have stolen a device from your home, gotten the log in information from someone who has been on your network, or even have successfully managed to hack into the network. In any case, there is a way to prevent the attacker from being able to make changes to your router settings. This is important because with this capability, it would be possible for the attacker to deny you access to the wireless internet in your home if they had access to change settings such as the ones we have discussed in this topic. The setting that needs to change is the wireless administration feature of the router. Up to this point, we have been able to change the router's settings by logging in to the router while connected to the WiFi. Now, we will be changing the setting so that logging into the router will require the user to be connected via an Ethernet cable.

1.) Connect an Ethernet cable to an available port in the back of the router.
2.) Log into the router via the Gateway Address
3.) Select the access control portion of the settings
4.) Select the main wireless SSID
5.) Select disable wireless access control.



Once all of these changes have been made to your router's settings, your wireless network is much more secure. Attackers will no longer be able to use default login information to access your network. Even if they manage to get logged into your WiFi, they will not be able to change any administrator settings. There are many other settings on modern routers, and researching topics such as MAC Address filtering can help you to find more ways to increase the security of your home network. There will always be those people looking for new ways to gain access to networks illegally, and it is important to stay up to date with the latest ways to block their attempts.

CONCLUSION

After reading this thesis, you should have a much better understand of the types of malware and attacks that exist in the world today. You should also understand some of the simple steps to take when protecting yourself from these kinds of attacks. I hope you are able to use this guide to better secure the devices you have on your own network. It is important to keep in mind that with these steps are only a few of the ways that you can protect yourself from attackers. Not only are there more steps to learn, but gaining a more thorough understanding of the security topics can help you to understand the ways these attacks work. It is important to stay up to date on common types of malware, and continually check the status of the security on your devices.

Personally, the experience of researching and writing this guide has helped me gain a deeper knowledge about computer security, and has made it easier for me to explain more advanced tasks in a way that the average computer user can understand. This is important because during a career in an IT-related field, I will likely be in contact with users who only have a basic understanding of how to use a computer.

I hope you enjoyed reading my thesis as much as I enjoyed researching and writing it. I feel like this is one of the most useful projects I have ever done. I hope any person who has read through it is able to benefit from its content, in order to better protect themselves from many types of malware prevalent online today. Thank you for reading my thesis, I hope it helped.

Works Cited

Batchelder, Dennis. "Microsoft Security Intelligence Report." 17 (2014): n. pag. Web. 11 Mar. 2015.

"Changing the Linksys Router's Administrator Password." *Linksys Knowledge Base*. N.p., n.d. Web. 10 Mar. 2015.

Ciampa, Mark D. *CompTIA Security Guide to Network Security Fundamentals*. 5th ed. Boston: Cengage Learning, 2015. Print.

File, Thom, and Camille Ryan. "Computer and Internet Use in the United States: 2013." *Computer and Internet Use in the United States: 2013* (2014): 1-16. Nov. 2014. Web. Feb. 2015.

Goldsborough, Reid. "When Malware Slows You Down." *Teacher Librarian* 41.1 (2014): 59. Web. 26 Feb. 2015.

Heddings, Lowell. "Here's What Happens When You Install the Top 10 Download.com Apps." *How-To Geek*. N.p., 11 Jan. 2015. Web. 10 Feb. 2015.

"How to Secure Your Wireless Home Network." *WikiHow*. N.p., n.d. Web. 1 Mar. 2015.

Milošević, Nikola. "History of Malware." *ARXIV* (2014): n. pag. Web. 26 Feb. 2015.